03500.015945

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	:	Examiner: Not Assigned
Satoru WAKAO, et al.	)	
	:	Group Art Unit: 2612
Application No.: 09/987,832	)	
	:	
Filed: November 16, 2001	)	
	:	
For: IMAGE DATA VERIFICATION SYSTEM	)	January 28, 2002

The Commissioner for Patents
Washington, D.C. 20231

SUBMISSION OF PRIORITY DOCUMENTS

Sir:

In support of Applicants' claim for priority under 35 U.S.C. § 119, enclosed are certified copies of the following Japanese applications:

2000-351529, filed November 17, 2000; and 2001-346689, filed November 12, 2001.

Applicants' undersigned attorney may be reached in our Washington office by telephone at (202) 530-1010. All correspondence should continue to be directed to our address given below.

Respectfully submitted,

Attorney for Applicants
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
BLK\cmv
DC_MAIN 65321 v 1

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１１月１７日

出願番号
Application Number: 特願２０００－３５１５２９

出願人
Applicant(s): キヤノン株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年１２月 ７日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００１－３１０７１５７

【書類名】　特許願

【整理番号】　4253001

【提出日】　平成12年11月17日

【あて先】　特許庁長官殿

【国際特許分類】　H04N　5/00

【発明の名称】　検証データ変換装置、ディジタルデータ改竄検出システム、検証データ変換方法、ディジタルデータ改竄検出方法、データ検証システム及び記録媒体

【請求項の数】　35

【発明者】

【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

【氏名】　若尾　聡

【発明者】

【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

【氏名】　岩村　恵市

【特許出願人】

【識別番号】　000001007

【氏名又は名称】　キヤノン株式会社

【代理人】

【識別番号】　100090273

【弁理士】

【氏名又は名称】　國分　孝悦

【電話番号】　03-3590-8901

【手数料の表示】

【予納台帳番号】　035493

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705348

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　検証データ変換装置、ディジタルデータ改竄検出システム、検証データ変換方法、ディジタルデータ改竄検出方法、データ検証システム及び記録媒体

【特許請求の範囲】

【請求項１】　外部から入力される映像データと、該映像データの検証データと、映像データが生成された装置との間で共有する共有情報とに基づいて該映像データが改竄されていないかどうかを検証する検証処理部と、

秘密情報を用いて該映像データから２次検証データを生成する検証データ生成部とを有する検証データ変換装置。

【請求項２】　上記請求項１において、共有情報と秘密情報を格納する記憶部を有することを特徴とする検証データ変換装置。

【請求項３】　上記請求項１又は２において、映像データが改竄されていないかどうかを検証する時に、ハッシュ関数を用いることを特徴とする検証データ変換装置。

【請求項４】　上記請求項１～３のいずれか１項において、秘密情報は公開鍵暗号方式の秘密鍵であることを特徴とする検証データ変換装置。

【請求項５】　上記請求項１～４のいずれか１項において、公開鍵暗号方式の秘密鍵と公開鍵のペアを生成することを特徴とする検証データ変換装置。

【請求項６】　上記請求項１～５のいずれか１項において、映像データ、２次検証データ、及び公開鍵を出力する出力部を有することを特徴とする検証データ変換装置。

【請求項７】　共有情報を用いて該映像データに対する検証データを生成する検証データ生成部と、映像データと検証データとを少なくとも記憶するデータ記憶部と、該映像データと検証データを出力する出力部とを有する映像入力装置と、

映像入力装置からの映像データと検証データとに基づいて該映像データが改竄されていないかどうかを検証する検証処理部と、秘密情報を用いて２次検証データを生成する検証データ生成部とを有する検証データ変換装置と、

検証データ変換装置で生成された２次検証データと、検証データ変換装置で使用された秘密情報に対応する公開情報とに基づいて該映像データの改竄を検証する映像検証装置とを有することを特徴とするディジタルデータ改竄検出システム。

【請求項８】　上記請求項７において、映像入力装置は、共有情報を記憶する記憶部を有することを特徴とするディジタルデータ改竄検出システム。

【請求項９】　上記請求項７又は８において、映像入力装置は、映像を撮影する撮像部を有することを特徴とするディジタルデータ改竄検出システム。

【請求項１０】　上記請求項７～９のいずれか１項において、映像入力装置は、検証データを生成する時に、ハッシュ関数を用いることを特徴とするディジタルデータ改竄検出システム。

【請求項１１】　上記請求項７～１０のいずれか１項において、映像入力装置は、撮像した映像データと生成した検証データとを外部に出力する出力部を有することを特徴とするディジタルデータ改竄検出システム。

【請求項１２】　上記請求項７～１１のいずれか１項において、映像検証装置は、公開情報を外部から入力するための入力部を有することを特徴とするディジタルデータ改竄検出システム。

【請求項１３】　上記請求項７～１２のいずれか１項において、映像検証装置で用いられる公開情報は、公開鍵暗号方式の公開鍵であることを特徴とするディジタルデータ改竄検出システム。

【請求項１４】　上記請求項７～１３のいずれか１項において、映像入力装置と検証データ変換装置がインタフェース部をそれぞれ有し、一体の装置として動作することを特徴とするディジタルデータ改竄検出システム。

【請求項１５】　上記請求項７～１４のいずれか１項において、検証データ変換装置は、外部装置とのインタフェース部とデータ記憶部とデータ演算部とを少なくとも有することを特徴とするディジタルデータ改竄検出システム。

【請求項１６】　上記請求項７～１５のいずれか１項において、検証データ変換装置は、ICカードであることを特徴とするディジタルデータ改竄検出システム。

【請求項１７】　外部から入力される映像データと、該映像データの検証データと、映像データが生成された装置との間で共有する共有情報とに基づいて該映像データが改竄されていないかどうかを検証する検証処理ステップと、

秘密情報を用いて該映像データから２次検証データを生成する検証データ生成ステップとを有する検証データ変換方法。

【請求項１８】　上記請求項１７において、共有情報と秘密情報を格納する記憶ステップを有することを特徴とする検証データ変換方法。

【請求項１９】　上記請求項１７又は１８において、映像データが改竄されていないかどうかを検証する時に、ハッシュ関数を用いる演算ステップを有することを特徴とする検証データ変換方法。

【請求項２０】　上記請求項１７～１９のいずれか１項において、公開鍵暗号方式の秘密鍵と公開鍵のペアを生成するステップを有することを特徴とする検証データ変換方法。

【請求項２１】　上記請求項１７～２０のいずれか１項において、映像データ、２次検証データ、及び公開鍵を出力する出力ステップを有することを特徴とする検証データ変換方法。

【請求項２２】　共有情報を用いて該映像データに対する検証データを生成する検証データ生成ステップと、映像データと検証データとを少なくとも記憶するデータ記憶ステップと、該映像データと検証データを出力する出力ステップとを有する映像入力ステップと、

映像入力ステップからの映像データと検証データとに基づいて該映像データが改竄されていないかどうかを検証する検証処理ステップと、秘密情報を用いて２次検証データを生成する検証データ生成ステップとを有する検証データ変換ステップと、

検証データ変換ステップで生成された２次検証データと、検証データ変換ステップで使用された秘密情報に対応する公開情報とに基づいて該映像データの改竄を検証する検証ステップを有する映像検証ステップとを有することを特徴とするディジタルデータ改竄検出方法。

【請求項２３】　上記請求項２２において、映像入力ステップは、共有情報

を記憶する記憶ステップを有することを特徴とするディジタルデータ改竄検出方法。

【請求項２４】　上記請求項２２又は２３において、映像入力ステップは、映像を撮影する撮像ステップを有することを特徴とするディジタルデータ改竄検出方法。

【請求項２５】　上記請求項２２～２４のいずれか１項において、映像入力ステップは、検証データを生成する時に、ハッシュ関数を用いる演算ステップを有することを特徴とするディジタルデータ改竄検出方法。

【請求項２６】　上記請求項２２～２５のいずれか１項において、映像入力ステップは、撮像した映像データと生成した検証データとを外部に出力する出力ステップを有することを特徴とするディジタルデータ改竄検出方法。

【請求項２７】　上記請求項２２～２６のいずれか１項において、映像検証ステップは、公開情報を外部から入力するための入力ステップを有することを特徴とするディジタルデータ改竄検出方法。

【請求項２８】　上記請求項２２～２７のいずれか１項において、映像検証ステップで用いられる公開情報は、公開鍵暗号方式の公開鍵であることを特徴とするディジタルデータ改竄検出方法。

【請求項２９】　請求項１７～２８のいずれか１項に記載のステップをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項３０】　計算能力に応じて、映像データから演算処理負荷の少ない１次検証データを生成する１次検証データ生成装置と、

該１次検証データを検証後、映像データから演算処理負荷の大きい２次検証データを生成する２次検証データ生成装置と、

映像データと該２次検証データとを用いて該映像データの改竄検出を行う検証装置とを有することを特徴とするデータ検証システム。

【請求項３１】　上記請求項３０において、１次検証データ生成時と１次検証データ検証時に共有情報を用いることを特徴とするデータ検証システム。

【請求項３２】　上記請求項３０又は３１において、２次検証データ生成時

に秘密情報を用いることを特徴とするデータ検証システム。

【請求項３３】　上記請求項３０～３２のいずれか１項において、２次検証データ検証時に公開情報を用いることを特徴とするデータ検証システム。

【請求項３４】　上記請求項３２又は３３において、秘密情報は、公開鍵暗号方式の秘密鍵であり、公開情報は公開鍵暗号方式の公開鍵であることを特徴とするデータ検証システム。

【請求項３５】　上記請求項３０～３４のいずれか１項において、１次検証データ生成、検証時および２次検証データ生成、検証時にハッシュ関数を用いることを特徴とするデータ検証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、撮影対象の映像情報をディジタルデータに変換し、改竄検出用データをディジタルデータに付加することで該映像情報の改竄を検出する技術に関する。

【０００２】

【従来の技術】

近年、従来の銀塩写真や8mmフィルムに替わって、撮影した情報をディジタル化し、ディジタルデータとして記録媒体等に記録するディジタルカメラといった映像入力装置が実用化されている。これにより、撮影した情報そのものをパーソナルコンピュータを始めとする情報処理装置に移し、表示させることが可能になった。このような映像データを通信回線を利用することで全国どこでも瞬時に映像データを送信することも可能になった。そのため、事故処理で証拠写真を扱う保険会社や建築現場の進捗状況の記録を扱う建設会社においてディジタル映像データの利用が考えられている。

【０００３】

しかし一方で目覚しいデータ処理技術の進歩により、映像データを始めとしたディジタルデータの編集をフォトレタッチツールや動画編集ツール等の使用で容易に行うことが可能になった。そのため、ディジタル映像データの信頼性は従来

の銀塩写真等と比較して低く、証拠としての能力に乏しいという問題があった。そこで映像データの改ざん、偽造が行われていた場合にそれを検出するような映像入力装置、システムが提案されてきた。

【０００４】

例えば"DIGITAL CAMERA WITH APPRARATUS FOR AUTHENTICATION OF IMAGES PRODUCED FROM AN IMAGE "という名称の米国特許第5499294や"映像入力装置および映像入力システム"という名称の特許出願公開番号：特開平9-200730 によると映像入力装置に固有の秘密情報および該映像入力装置に接続される外部装置に固有の秘密情報の少なくても一方の情報と該映像入力装置にて撮影してディジタル化したディジタルデータとに基づき、所定の演算を実行して該ディジタルデータを識別する情報、すなわちディジタル署名データを生成し、該ディジタル署名データと映像入力装置にて撮影してディジタル化したディジタルデータとを映像入力装置の出力とするものである。また、上記公報ではディジタル署名データ生成にハッシュ関数と公開鍵暗号を使用している。公開鍵暗号については後で説明する。

【０００５】

ディジタル署名とは、送信者がデータと一緒に該データに対応する署名データを送り、受信者がその署名データを検証して該データの正当性を確認することである。

【０００６】

ディジタル署名データ生成にハッシュ関数と公開鍵暗号を用いたデータの正当性の確認は以下のようになり、これが上記公報の方法である。

【０００７】

秘密鍵をKs，公開鍵をKpとすると発信者は、平文データMをハッシュ関数により圧縮して一定長の出力h を算出する演算を行う。次に秘密鍵Ksでh を変換してディジタル署名データｓを作成する演算すなわちＤ(Ks,h) ＝ｓを行う。その後、該ディジタル署名データｓと平文データMとを送信する。一方受信者は受信したディジタル署名データｓを公開鍵Kp で変換する演算すなわちE(Kp,s)= E(Kp,D(Ks,h''))= h''と、受信した平文データM'を発信者と同じハッシュ関数により圧

縮してh’ を算出する演算を行い、h’とh’’が一致すれば受信したデータM’を正当であると判断する。

【０００８】

平文データMが送受信間で改ざんされた場合にはE(Kp,s)= E(Kp,D(Ks,h’’))= h’’と、受信した平文データM’を発信者と同じハッシュ関数により圧縮したh’が一致しないので改ざんを検出できる。ここで、平文データMの改ざんに合わせてディジタル署名データｓの改ざんも行われてしまうと改ざんの検出ができなくなる。しかし、これはhから平文データMを求める必要があり、このような計算はハッシュ関数の一方向性により不可能である。

【０００９】

次にハッシュ関数について説明する。ハッシュ関数は上記ディジタル署名の生成を高速化するため等に用いられる。ハッシュ関数は任意の長さの平文データMに処理を行い、一定の長さの出力hを出す機能を持つ。ここで、出力hを平文データMのハッシュ値（またはメッセージダイジェスト、ディジタル指紋）という。ハッシュ関数に要求される性質として、一方向性と衝突耐性が要求される。一方向性とはｈを与えた時、h=H(M)となる平文データMの算出が計算量的に困難であることである。衝突耐性とは平文データMを与えた時、H(M)=H(M’)となる平文データM’(M≠M’)の算出が計算量的に困難であること及びH(M)=H(M’)かつM≠M’となる平文データM,M’の算出が計算量的に困難であることである。

【００１０】

ハッシュ関数としてはMD-2,MD-4,MD-5,SHA-1,RIPEMD-128,RIPEMD-160等が知られており、これらのアルゴリズムは一般に公開されている。

【００１１】

続いて公開鍵暗号について説明する。公開鍵暗号は暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。公開鍵暗号の特徴としては、

(a) 暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

(b) 各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密

に記憶しておけばよい。

(c) 送られてきた通信文の送信者が偽者でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

が挙げられる。

【００１２】

例えば、平文データ M に対して、公開の暗号鍵 kp を用いた暗号化操作をE(Kp,M) とし、秘密の復号鍵 Ksを用いた復号操作を D(Ks,M) とすると、公開鍵暗号アルゴリズムは、まず次の2つの条件を満たす。

【００１３】

(1) Kp が与えられたとき、E(Kp,M) の計算は容易である。Ksが与えられたとき、D(Ks,M) の計算は容易である。

(2) もし Ksを知らないなら、Kp と E の計算手順と C＝E(Kp,M) を知っていても、M を決定することは計算量の点で困難である。

【００１４】

次に、上記(1)、(2)に加えて、次の(3)の条件が成立することにより秘密通信が実現できる。

(3) 全ての平文データ M に対し、E(Kp,M) が定義でき、D(Ks,E(Kp,M))＝Mが成立する。つまり、Kp は公開されているため誰もが E(Kp,M) を計算することができるが、 D(Ks,E(Kp,M)) を計算して M を得ることができるのは秘密鍵 Ksを持っている本人だけである。一方、上記(1)、(2)に加えて、次の(4)の条件が成立することにより認証通信が実現できる。

【００１５】

(4) すべての平文データM に対し、D(Ks,M) が定義でき、E(Kp,D(Ks,M))＝Mが成立する。つまり、D(Ks,M) を計算できるのは秘密鍵 Ksを持っている本人のみであり、他の人が偽の秘密鍵 Ks ' を用いて D(Ks',M) を計算し Ks を持っている本人になりすましたとしても、E(Kp,D(Ks',M))≠M なので受信者は受けとった情報が不正なものであることを確認できる。また、D(Ks,M) が改ざんされても E(Kp,D(Ks,M)')≠M となり、受信者は受けとった情報が不正なものであることを確認できる。

【００１６】

上記の秘密通信と認証通信とを行うことができる代表例としてRSA暗号やR暗号やW暗号等が知られている。

【００１７】

ここで、現在最も使用されているRSA暗号の暗号化、復号は次式で示される。

暗号化：暗号化鍵（e,n)　暗号化変換$C=M^{e}(\mathrm{mod}\ n)$

復号：復号鍵（d,n)　復号変換$M=C^{d}(\mathrm{mod}\ n)$

n=p・q　ここでp、q　は大きな異なる素数

【００１８】

上記のように、RSA暗号は暗号化にも復号にもべき乗演算と剰余演算が必要であるので、DESをはじめとする共通鍵暗号と比較すると演算量が膨大なものとなり高速な処理は難しい。

【００１９】

【発明が解決しようとする課題】

しかし、該公開鍵暗号を用いたディジタル署名データ生成を該映像入力装置で行う場合、処理時間がかかるか、処理時間を速くする場合には、映像入力装置のCPU（中央演算処理装置）、メモリ（記録媒体）といったハードウエア上の能力を向上させる必要がある。しかしこの向上は結果として製品のコストアップの要因となり好ましくない。

【００２０】

これは、映像入力装置の演算リソース（CPU（中央演算処理装置）、メモリ（記録媒体））は映像データの撮影時の処理等のみに使用されることを前提に設計されているものであるため、これらのリソースをディジタル署名データ生成の処理に振り分ける余地が少ないこと、及び公開鍵暗号方式は共通鍵暗号方式に比較して多く計算を必要とするためによるものである。

【００２１】

代表的な公開鍵暗号方式として前述のRSAがあるが、前に記述したようにこの方式はべき乗演算と剰余演算が必要であるために演算処理が複雑となり、DESをはじめとする共通鍵暗号方式の数百倍から数千倍の処理時間が必要であるとされ

ている。従って、豊富な演算リソースを有しない映像入力装置で撮影した映像データの完全性（データの改竄が行われていないこと）を保証するためのデータをいかにして生成するかという問題がある。

【００２２】

また、上記にて生成した完全性を保証するためのデータを基にして何処の装置で、何時、どのように検証を行うかといった、検証システム全体をどのように構築するのかといった問題もある。さらには、該完全性を保証するために生成されたデータを用いて、映像データの完全性を検証する時に必要となる情報の存在場所の明示方法や映像データをどのように管理すれば効率的に管理ができるかといった問題がある。

【００２３】

本発明の目的は、豊富な演算リソースを持たない映像入力装置の能力を向上させることなく、該映像入力装置にて撮影した映像データの完全性を保証するためのデータを生成することであり、さらには、該映像データに関するデータを（映像データと）関連付けることでデータベースを作成して管理等を容易にし、トータルな映像データの認証システムを構築することである。

【００２４】

【課題を解決するための手段】

本発明の一観点によれば、外部から入力される映像データと、該映像データの検証データと、映像データが生成された装置との間で共有する共有情報とに基づいて該映像データが改竄されていないかどうかを検証する検証処理部と、秘密情報を用いて該映像データから２次検証データを生成する検証データ生成部とを有する検証データ変換装置が提供される。

【００２５】

本発明の他の観点によれば、共有情報を用いて該映像データに対する検証データを生成する検証データ生成部と、映像データと検証データとを少なくとも記憶するデータ記憶部と、該映像データと検証データを出力する出力部とを有する映像入力装置と、映像入力装置からの映像データと検証データとに基づいて該映像データが改竄されていないかどうかを検証する検証処理部と、秘密情報を用いて

２次検証データを生成する検証データ生成部とを有する検証データ変換装置と、検証データ変換装置で生成された２次検証データと、検証データ変換装置で使用された秘密情報に対応する公開情報とに基づいて該映像データの改竄を検証する映像検証装置とを有することを特徴とするディジタルデータ改竄検出システムが提供される。

【００２６】

本発明のさらに他の観点によれば、外部から入力される映像データと、該映像データの検証データと、映像データが生成された装置との間で共有する共有情報とに基づいて該映像データが改竄されていないかどうかを検証する検証処理ステップと、秘密情報を用いて該映像データから２次検証データを生成する検証データ生成ステップとを有する検証データ変換方法が提供される。

【００２７】

本発明のさらに他の観点によれば、共有情報を用いて該映像データに対する検証データを生成する検証データ生成ステップと、映像データと検証データとを少なくとも記憶するデータ記憶ステップと、該映像データと検証データを出力する出力ステップとを有する映像入力ステップと、映像入力ステップからの映像データと検証データとに基づいて該映像データが改竄されていないかどうかを検証する検証処理ステップと、秘密情報を用いて２次検証データを生成する検証データ生成ステップとを有する検証データ変換ステップと、検証データ変換ステップで生成された２次検証データと、検証データ変換ステップで使用された秘密情報に対応する公開情報とに基づいて該映像データの改竄を検証する検証ステップを有する映像検証ステップとを有することを特徴とするディジタルデータ改竄検出方法が提供される。

【００２８】

本発明のさらに他の観点によれば、計算能力に応じて、映像データから演算処理負荷の少ない１次検証データを生成する１次検証データ生成装置と、該１次検証データを検証後、映像データから演算処理負荷の大きい２次検証データを生成する２次検証データ生成装置と、映像データと該２次検証データとを用いて該映像データの改竄検出を行う検証装置とを有することを特徴とするデータ検証シス

テムが提供される。

【００２９】

本発明によれば、豊富な演算リソースを持たない映像入力装置の能力を向上させることなく、該映像入力装置にて撮影した映像データの完全性を保証するためのデータを生成することができる。

【００３０】

【発明の実施の形態】

以下、本発明の実施形態を、実施例に沿って図面を参照しながら説明する。

映像データの改竄を検出するためのシステムを構成する映像入力装置、検証データ変換装置、映像検証装置の構成について図１～３に基づいて説明し、次に映像データの改竄検出システムにおける装置間の処理に関して図４に基づいて説明し、続いて各装置の処理フローに関して図９～１１に基づいて説明する。

【００３１】

映像入力装置の構成

図１は、本発明における実施例の映像入力装置の構成を示す図であり、図における各ブロックは機能別の構成要素である。制御/演算部１１は撮影指示がなされると、ROM１７にあらかじめ格納されているプログラムに従い映像データの圧縮処理、検証データ生成等の各種演算処理を行う。駆動部１２は撮影に必要な機械的な動作を制御/演算部１１の制御のもとで行う。作業用メモリ１３では映像データが一時的に保管され、ここで該映像データの圧縮及び各種演算処理が行われる。

【００３２】

光学系１４は電荷結合素子CCDまたは光学センサーを含み、撮影指示がなされると被写体の撮影、電気信号処理、ディジタル信号処理等を行う。保管用メモリ１５は処理済の映像データを格納する。

【００３３】

外部装置とのインタフェース部１６はメモリカード、携帯端末、通信装置といった外部装置とのインタフェースであり、映像データや検証データをこれらの機器へ送信する時に使用される。

【００３４】

ROM１７は読み出し専用メモリであり、あらかじめ動作プログラムや検証データ生成に必要な共有情報が格納される。操作部１８は撮影者の撮影指示をはじめとする各種の指示を受け付けるためのものである。

【００３５】

検証データ変換装置の構成

図２は、本発明における実施例の検証データ生成装置の構成を示す図であり、図における各ブロックは機能別の構成要素である。

【００３６】

インタフェース部２４は映像入力装置、映像検証装置といった外部装置とのインタフェースであり、検証データが挿入された映像データや該映像データの検証に必要となる共有情報や、２次検証データ生成に必要となる秘密情報を受信する時、さらには、２次検証データが挿入された映像データを送信する時に使用され、受信した映像データや共有情報は保管用メモリ２５に、格納される。

【００３７】

入力された映像データの検証指示が操作部２７に対してなされると、ROM２６にあらかじめ格納されているプログラムに従い検証データの検証処理を作業用メモリ２３にて行う。該検証処理に必要になる共有情報はあらかじめROM２６に格納されていて必要時にROM２６から作業用メモリ２３に読み込まれるか、外部インタフェース部２４を通して外部の装置から作業用メモリ２３に読み込まれる。検証の結果、映像データの改竄が為されていないと判断した場合には引き続いて２次検証データ生成が映像データと保管用メモリ２５に格納されている秘密情報とを用いて行われる。該秘密情報は、あらかじめ保管用メモリ２５に格納されているか、制御/演算部２１の指示により作業用メモリ２３にて生成された後に保管用メモリ２５に格納されるか、さらには、外部装置から受信して保管用メモリ２５に格納される。

【００３８】

ROM２６は読み出し専用メモリであり、あらかじめ検証プログラム、２次検証データ生成プログラムが格納される。操作/入力部２７は起動指示、検証指示を

はじめとするユーザからの各種指示を受け付けるためのものである。

【００３９】

作業用メモリ２３では受信した映像データが保管用メモリ２５から移され、ここで該映像データの検証処理、２次検証データ生成及び各種演算処理が行われる。出力部２２は、検証処理結果をディスプレイやプリンタといった外部の装置に出力する。

【００４０】

映像検証装置の構成

図３は、本発明における実施例の映像検証装置の構成を示す図であり、図に示される各ブロックは機能別の構成要素である。

【００４１】

インタフェース部３４は映像データ検証装置といった外部装置とのインタフェースであり、映像データや、映像データの検証に必要となる秘密情報に対応する公開情報を受信する時に使用される。

【００４２】

入力された映像データの検証指示が操作部３７に対してなされると、ROM３６にあらかじめ格納されているプログラムに従って、制御／演算部３１が映像データに付加されている検証データの検証処理を作業用メモリ３３にて行う。該検証処理に必要になる公開情報はあらかじめROM３６に格納されていて必要時にROM３６から作業用メモリ３３に読み込まれるか、外部インタフェース部３４を通して外部の装置から作業用メモリ３３に読み込まれる。

【００４３】

ROM３６は読み出し専用メモリであり、あらかじめ検証プログラムが格納される。操作/入力部３７は起動指示、検証指示をはじめとするユーザからの各種指示を受け付けるためのものである。

【００４４】

作業用メモリ３３では受信した映像データが保管用メモリ３５から移され、ここで該映像データの検証処理及び各種演算処理が行われる。出力部３２は、検証処理結果をディスプレイやプリンタといった外部の装置に出力する。

【００４５】

受信した映像データに対して、改竄の有無、改竄検出に必要となる公開情報のありか、どの検証データ変換装置から送られてきたものか、登録日時、検証日時等の情報を関連付けてデータベースを作成し、保管用メモリ３５に記憶する。

【００４６】

図４は、本実施例における、各装置の処理を示す図である。以下では図４中の（１）から（１１）の番号と以下の（１）から（１１）の番号とを対応させて説明する。映像入力装置における検証データ生成処理は、図５に示すように映像データに対して、共有情報との排他的論理和演算といった簡易な演算を行った後、ハッシュ関数による演算を行い、その出力を検証データとする方式とする。該検証データは検証データ変換装置において該共有情報を用いて検証後、公開鍵暗号演算を用いて生成した２次検証データと差し替えられる。該２次検証データは、映像検証装置において、公開鍵暗号演算を用いて検証される。

【００４７】

（１）映像入力装置で被写体を撮影すると撮影された映像データは、電気信号処理、ディジタル信号処理等が行われる。上記処理後、映像圧縮処理が行われてからファイルフォーマット化される。代表的な映像圧縮方式としては、JPEG（静止画）、MPEG（動画）等が有名であり、ファイルフォーマットとしては、JFIF,TIFF,GIFF（静止画）が有名である。映像圧縮処理後、該圧縮された映像データがROMに格納されている共有情報を用いて処理が行われて検証データが生成される。該処理について図６を用いて説明する。

【００４８】

ここでは、映像入力装置の共有情報として例えば”11111111”を考える。これは、映像入力装置の装置外に公開されずかつ検証データ変換装置と共有できればどのようなものでよい。またこの共有情報は、容易に外部へ情報が漏れないように管理する。上記映像データの所定位置のバイトと、秘密情報である”11111111”とのビット毎の排他的論理和演算が行われて中間データとなる。ここで、所定位置のバイトとして最上位バイトとする。但し、この所定位置のバイトとしては任意の位置とすることもできる。さらに、中間データの生成の演算として映像データ

と共有情報のビット毎の排他的論理和演算としたが、演算出力がこれら２つのデータのみに基づいて生成され、高速に処理可能なものであればどのような演算でもよい。最後に、中間データを入力としてハッシュ関数の演算処理が行われる。該処理で出力される値が検証データとなる。ハッシュ関数としては、MD-5,SHA-1が特に有名であり、MD-5のハッシュ値は128ビットであり、SHA-1は160ビットである。従って、ハッシュ関数としてMD-5を採用すれば検証データは128ビットとなり、SHA-1を採用すれば160ビットとなる。該処理で得られた検証データは映像データと共有情報に固有の情報となり、改ざん者は入力である映像データを改ざんしても共有情報を知らないので、該映像データに対応する検証データを得ることができない。これはハッシュ関数の一方向性により、得られたハッシュ値からその元のデータを知ることができない、すなわち共有情報を知ることができないことから保証されるためである。よって、秘密情報を知らない改ざん者は映像データの改ざんが不可能になる。該検証データは、秘密情報がROMから外部に流出しない限り安全であることは、上記にて説明した通りである。

【００４９】

（２）生成された検証データは、ファイルフォーマット化された映像データのヘッダ部の部分に挿入される。一例としてJFIF方式にてフォーマット化された映像データのヘッダ部に挿入されるデータ構成例を図７に示す。挿入されるデータは、識別子エリア、長さエリア、検証データエリアで構成される。識別子エリアには、ここからヘッダ部が始まること示すデータ（マーカ）が記述され、長さエリアには、長さエリアと検証データエリアとの合計のデータ長がバイト単位で記述され、検証データエリアには、上記で生成された検証データが記述される。映像データを再生（表示）する時にはこのヘッダ部は読み飛ばされるので、データを挿入することで画質の劣化、画像の変化が発生することはない。

【００５０】

（３）検証データが挿入された映像データは、外部装置とのインタフェース部においてデータ変換された後に送出される。外部装置がネットワークである場合には、そのプロトコルに応じたデータ変換が行われ、外部装置がフロッピーディスク、メモリカード等の記録デバイスである場合には、該デバイスにデータの記

録が行われる。

【００５１】

（４）映像データを受け取った検証データ変換装置は、最初に映像データのヘッダ部の検証データを抽出する。次に映像データからディジタル署名データを含むヘッダ部を削除し、ヘッダ部を削除した映像データから上記（１）と同様にして検証データを生成する。上記（１）においては、映像データに対して共有情報（”11111111”）との排他的論理和演算を行った後、ハッシュ関数による演算をおこなったので、ここでも同様の演算を行う。

【００５２】

（５）該演算結果と映像データのヘッダ部から抽出された検証データとを比較する。２つのデータが一致した場合には、映像入力装置から検証データ変換装置の間で改竄が行われていないと判断し、映像データの２次検証データ生成処理を行う。一致しない場合には、改竄が行われたと判断しその結果を出力する（２次検証データ生成処理は行わない）。

【００５３】

（６）上記の比較処理にて改竄が行われていないと判断した場合には、２次検証データ生成処理を行う。該生成処理は、図８に示すように映像データ（受け取った映像データからヘッダ部を削除したデータ）に対して、ハッシュ関数による演算を行いダイジェストデータを生成し、次に該ダイジェストデータに対して秘密情報を鍵とする公開鍵暗号演算を行い、その出力を２次検証データとするものである。ここで、使用した秘密情報は、あらかじめ検証データ変換装置に組み込んでおいてもいいし、検証データ変換装置内部で生成して保持してもよい。公開鍵暗号演算として例えばRSA演算を用いる場合には、秘密鍵と公開鍵は以下のように生成される。

【００５４】

まず、任意の相異なる２つの大きな素数p,qを生成するとともにその積n = p・qを計算する。次に、(p-1)と(q-1)の最小公倍数Lを計算し、Lと互いに素でLより小さい任意の整数eを生成する。最後に次式を満たす整数dを計算する。ed = 1(mod L)。公開鍵を（e,n）とし秘密鍵を（d,n）とする。上記では、公開鍵暗号演

算としてRSA演算を用いる場合について説明したが、これに限るものではなく、公開鍵暗号演算が行えるようなものであればどのようなものでもよい。

【００５５】

検証データ変換装置には、PCといった映像検証装置よりも計算リソースが豊富な機器を使用することで、演算負荷の大きい公開鍵暗号演算を高速に処理することが可能になる。

【００５６】

（７）生成された２次検証データは、（２）と同様に映像データのヘッダ部に挿入（検証データと差し替え）される。２次検証データが挿入された映像データは、（３）と同様に外部装置とのインタフェース部においてデータ変換された後に送出される。

【００５７】

（８）映像データを受け取った映像検証装置は、最初に映像データのヘッダ部の２次検証データを抽出する。次に抽出した２次検証データに対して、検証データ変換装置で使用された秘密情報に対応する公開情報を鍵とする公開鍵暗号演算を行いダイジェストデータを生成する。

【００５８】

（９）映像データから２次検証データを含むヘッダ部を削除し、ヘッダ部を削除した映像データから上記（６）と同様にしてハッシュ関数によりダイジェストデータを生成する

【００５９】

（１０）上記（８）で生成したダイジェストデータと、上記（９）で生成したダイジェストデータとを比較して２つのデータが一致した場合には検証データ変換装置から映像検証装置の間で改竄が行われていないと判断し、その旨の表示を行う。一方で、一致しない場合には改竄が行われたと判断しその旨の表示を行う。

【００６０】

（１１）検証データ変換装置からの映像データに対して、改竄の有無、改竄検出に必要となる公開情報のありか、どの検証データ変換装置から送られてきたも

のか、登録日時、検証日時等の情報を関連付けてデータベースを作成する。このようなデータベースを作成することで、撮影された映像データの管理を行う。

【００６１】

本実施例では、映像入力装置での検証データ生成の方式として、「映像データに対して、共有情報との排他的論理和演算を行った後ハッシュ関数による演算を行い、その出力を検証データとする」ものであったが、演算リソースの少ない装置でも現実的な時間で処理できる演算方法であれば、これに限るものではない。

【００６２】

このように本方式は、映像入力装置において剰余算やべき乗演算といった処理を行わないために、公開鍵暗号演算を用いる場合と比較して高速に検証のためのデータを生成できることが特徴である。すなわち演算能力の乏しい装置でも検証データを生成できる。また、本方式の処理の流れは、豊富な演算リソースを持たない映像入力装置において簡易な演算による検証データを生成し、次に豊富な演算リソースを有する検証データ変換装置において公開鍵暗号を用いた２次検証データを生成し、検証データを２次検証データに差し替える。最後に映像検証装置では該２次検証データを用いて改竄の検出を行う。このような演算リソースに応じた一連の処理をそれぞれの装置で行うことで、システム全体で安全な改竄検出方法が提供可能となる。

【００６３】

豊富な演算リソースを持たない映像入力装置において生成した検証データ（映像データに対して、共有情報との排他的論理和演算を行った後、ハッシュ関数演算を行い、その出力）を用いて映像検証装置において改竄の検出を行うといった方式の場合には、該映像入力装置で使用した共有情報を用いることが必要になるが、該共有情報は２つの装置間のみが知りうる秘密とすることが必須である。もしも該共有情報が改竄者に漏れた場合には、共有情報を用いて検証データを偽造できるので映像データの改竄が可能になる。すなわち、共有情報をどのように２装置間で秘密裏に配送または共有するかという問題がある。

【００６４】

一方で、２次検証データを用いて映像検証装置で改竄の検出を行う本方式の場

合には、上記のような共有情報の配送、共有の問題は発生しない。これは、一般の誰にでも公開できる公開情報（公開鍵）を用いて検証を行うためである。

【００６５】

本方式により豊富な演算リソースを持たない映像入力装置の能力を向上させることなく、該映像入力装置にて撮影した映像データの完全性を、秘密に保持する必要がなく、鍵配送の問題がない公開情報（検証データ変換装置で２次検証データを生成する時に使用した秘密情報に対応する情報）を用いるだけで検証可能になった。さらには、該映像データに関するデータを（映像データと）関連付けることでデータベースを作成して管理等を容易にすることができ、トータルな映像データの認証システムを構築することが可能になった。

【００６６】

以下では本実施例における映像入力装置の動作の一例について図９のフローチャートを用いて説明する。

【００６７】

図９は、撮影した映像データに対して共有情報を用いて検証データを生成した後、該検証データを映像データに挿入する処理を説明するためのフローチャートである。

【００６８】

図９において、ステップ９１では、被写体の撮影、電気信号処理及びディジタル信号処理、圧縮処理等が行われてフォーマット化された映像データが生成される。

【００６９】

次に、ステップ９２では、上記ステップ９１で生成された映像データに対して、共有情報との排他的論理和演算を行った後、ハッシュ関数による演算を行い検証データを生成する。

【００７０】

次に、ステップ９３では、上記ステップ９２で生成された検証データが映像データのヘッダ部に挿入される。

【００７１】

次に、ステップ９４では、上記検証データが挿入された映像データに対して送信処理が行われて送出される。該処理は、映像検証装置との間がネットワークで接続されている場合には、該ネットワークにて使用されているプロトコルに応じた変換であり、映像検証装置との間がネットワークで接続されておらず、メモリカード等の記憶媒体でデータのやりとりが行われる場合には記憶媒体への記録となる。

【００７２】

ここで、１回の撮影毎に、１枚の映像データに対して検証データを生成/挿入する処理をおこなっても良いし、撮影終了後に、撮影した１枚、１枚の各映像データに対して検証データを生成/挿入する処理をまとめて行っても良い。

【００７３】

以下では本実施例における検証データ変換装置の動作の一例について図１０のフローチャートを用いて説明する。

【００７４】

図１０は、検証データが挿入された映像データを受信し、映像入力装置と共有する共有情報を用いて映像データの検証および新しい検証データの生成処理を説明するためのフローチャートである。

【００７５】

図１０において、ステップ１０１では、検証データが挿入された映像データを映像入力装置から受信する。映像入力装置との間がネットワークで接続されている場合には、ネットワークから該映像データを受信し、映像入力装置との間がネットワークで接続されておらず、メモリカード等の記憶媒体でデータのやりとりが行われる場合には記憶媒体経由で受け取る。

【００７６】

次に、ステップ１０２では、ステップ１０１で受信した映像データのヘッダ部から該映像データに挿入されている検証データを抽出する。

【００７７】

次に、ステップ１０３では、ヘッダ部を削除した映像データから上記ステップ９２と同様に、排他的論理和演算とハッシュ関数による演算を行い検証データを

生成する。

【００７８】

次に、ステップ１０４では、ステップ１０３で生成した検証データとステップ１０２で抽出した検証データが一致するかが判断され、一致する場合には、ステップ１０５に進み、一致しない場合にはステップ１０６に進む。

【００７９】

次に、ステップ１０６では、映像データが改竄されたことを意味するメッセージを出力し動作を終了する。

【００８０】

ステップ１０５では、映像データ（受け取った映像データからヘッダ部を削除したデータ）に対して、ハッシュ関数による演算を行いダイジェストデータを生成し、さらに該ダイジェストデータに対して秘密情報を鍵とする公開鍵暗号演算を行うことで２次検証データを生成する。ここで、使用した秘密情報は、あらかじめ検証データ変換装置に組み込んでおいてもいいし、検証データ変換装置内部で生成して保持してもよい。

【００８１】

ステップ１０７では、生成された２次検証データがステップ９３と同様に映像データのヘッダ部に挿入された後、外部装置とのインタフェース部においてデータ変換された後に送出される。

【００８２】

以下では本実施例における映像検証装置の動作の一例について図１１のフローチャートを用いて説明する。

【００８３】

図１１は、検証データが挿入された映像データを受信し、検証データ変換装置が２次検証データ生成の際に用いた秘密情報に対応する公開情報を用いて該映像データの検証を説明するためのフローチャートである。

【００８４】

図１１において、ステップ１１１では、検証データが挿入された映像データを受信する。ネットワークで接続されている場合には、ネットワークから該映像デ

ータを受信し、ネットワークで接続されておらず、メモリカード等の記憶媒体でデータのやりとりが行われる場合には記憶媒体経由で受け取る。

【００８５】

次に、ステップ１１２では、検証データ変換装置が検証データ生成の際に用いた秘密情報に対応する公開情報を取得する。秘密情報と公開情報が該検証データ変換装置にて生成された場合には、検証データ変換装置から取得し、あらかじめ秘密情報が検証データ変換装置に組み込まれているような場合には、該秘密情報に対応する公開情報を公開しているサーバ等の装置から取得する。

【００８６】

次にステップ１１３では、上記ステップ１１１で受け取った映像データのヘッダ部に存在する２次検証データを抽出する。

【００８７】

次にステップ１１４では、上記ステップ１１３にて抽出した２次検証データに対して、ステップ１１２にて取得した公開情報を鍵とする公開鍵暗号演算を行いダイジェストデータを生成する。

【００８８】

次にステップ１１５では、上記ステップ１１１で受け取った映像データから２次検証データを含むヘッダ部を削除し、ヘッダ部を削除した映像データからハッシュ関数による演算を行いダイジェストデータを生成する。

【００８９】

次にステップ１１６では、上記ステップ１１４と１１５で生成したダイジェストデータを比較し、２つのダイジェストデータが一致する場合には、ステップ１１７に進み、一致しない場合にはステップ１１８に進む。

【００９０】

次にステップ１１７では、ダイジェストデータが一致しなかったことは、映像データに対して改竄が行われたことを意味するので、映像データが改竄されたことを意味するメッセージを出力し動作を終了する。

【００９１】

次にステップ１１８では、ダイジェストデータが一致したことは、映像データ

に対して改竄が行われていないことを意味するので、映像データが改竄されていないことを意味するメッセージを出力する。

【００９２】

次にステップ１１９では、改竄の有無、改竄検出に必要となる公開情報のありか、どの検証データ変換装置から送られてきたものか、登録日時、検証日時等の情報を映像データと関連付けてデータベースを作成して処理を終了する。

【００９３】

本実施例により豊富な演算リソースを持たない映像入力装置の性能を向上させることなく、該映像入力装置にて撮影した映像データの完全性を、秘密に保持する必要のない公開情報を用いるだけで検証可能になった。

【００９４】

上記実施例の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って動作させることによって実施したものも、本発明の範疇に含まれる。

【００９５】

この場合、上記ソフトウェアのプログラムコード自体が上述した実施例の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００９６】

なお、上記実施例は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【００９７】

【発明の効果】

以上説明したように本発明によれば、豊富な演算リソースを持たない映像入力装置の能力を向上させることなく、該映像入力装置にて撮影した映像データの完全性を保証するためのデータを生成することができる。

【図面の簡単な説明】

【図１】

本発明に係わる実施例における、映像入力装置の構成を示すブロック図である。

【図２】

本発明に係わる実施例における、検証データ変換装置の構成を示すブロック図である。

【図３】

本発明に係わる実施例における、映像検証装置の構成を示すブロック図である。

【図４】

本発明に係わる実施例における、映像データ検証のためのシステムを示す図である。

【図５】

本発明に係わる実施例における、検証データの生成法の一例を示す図である。

【図６】

本発明に係わる実施例における、検証データの生成法の一例の詳細を示す図である。

【図７】

本発明に係わる実施例における、映像データに挿入されるデータの構成例を示す図である。

【図８】

本発明に係わる実施例における、２次検証データの生成法の１つを示す図である。

【図９】

本発明に係わる実施例における、映像入力装置の動作を説明するためのフローチャート図である。

【図１０】

本発明に係わる実施例における、検証データ変換装置の動作を説明するためのフローチャート図である。

【図１１】

本発明に係わる実施例における、映像データ検証装置の動作を説明するためのフローチャート図である。

【符号の説明】

１１　制御／演算部

１２　駆動部

１３　作業用メモリ

１４　光学系

１５　保管用メモリ

１６　インタフェース部

１７　ＲＯＭ

１８　操作部

２１　制御／演算部

２２　出力部

２３　作業用メモリ

２４　インタフェース部

２５　保管用メモリ

２６　ＲＯＭ

２７　操作／入力部

３１　制御／演算部

３２　出力部

３３　作業用メモリ

３４　インタフェース部

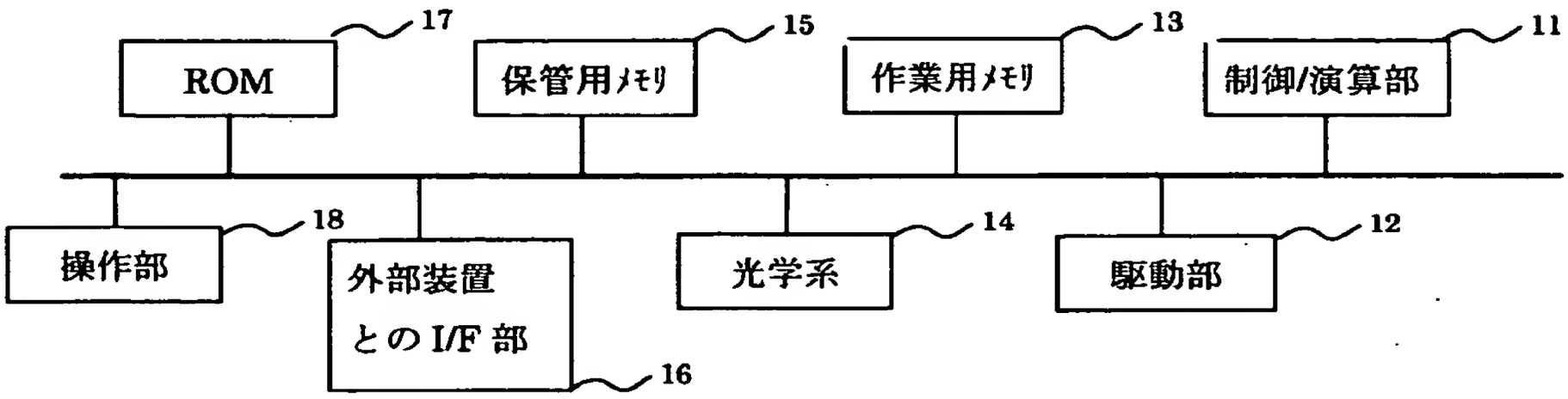
３５　保管用メモリ

３６　ＲＯＭ

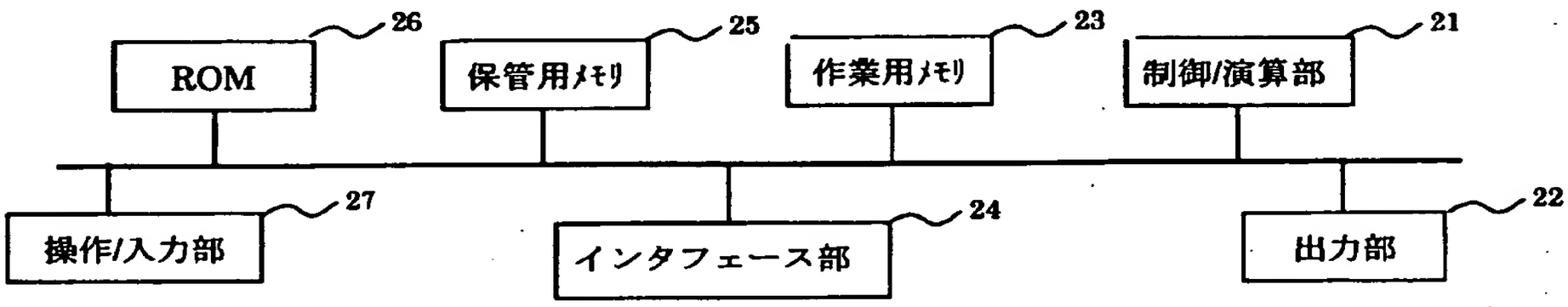
３７　操作／入力部

【書類名】　　図面

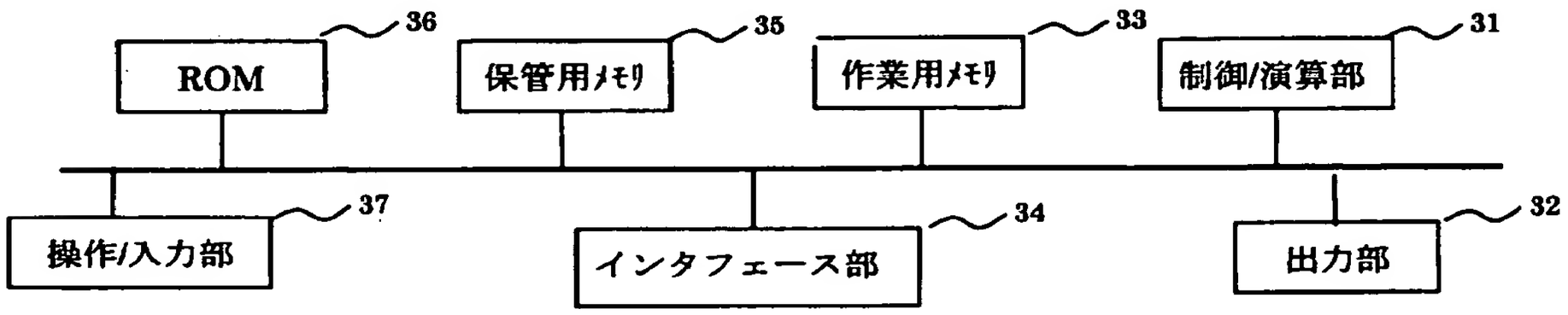
【図１】



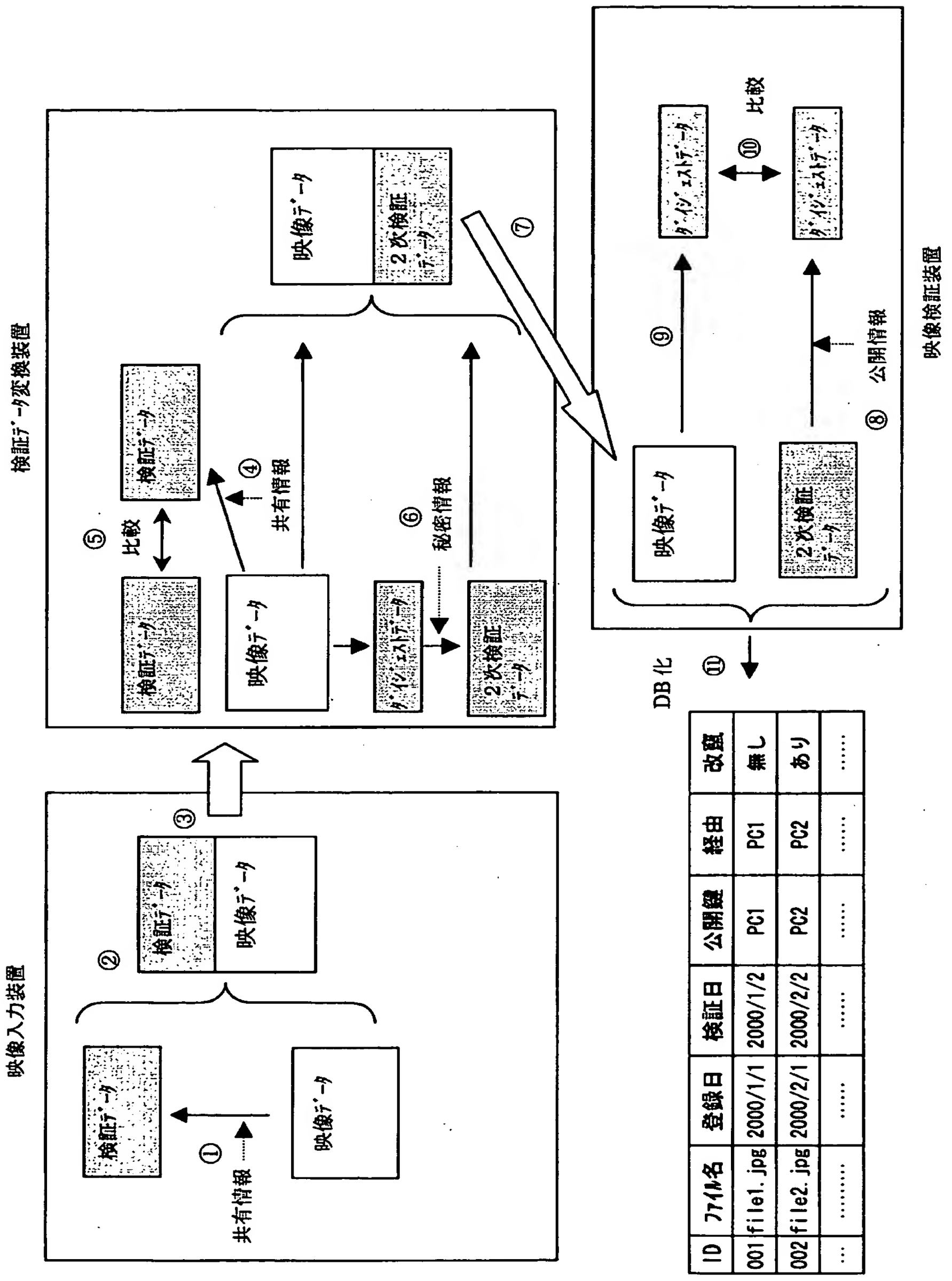
【図２】



【図３】

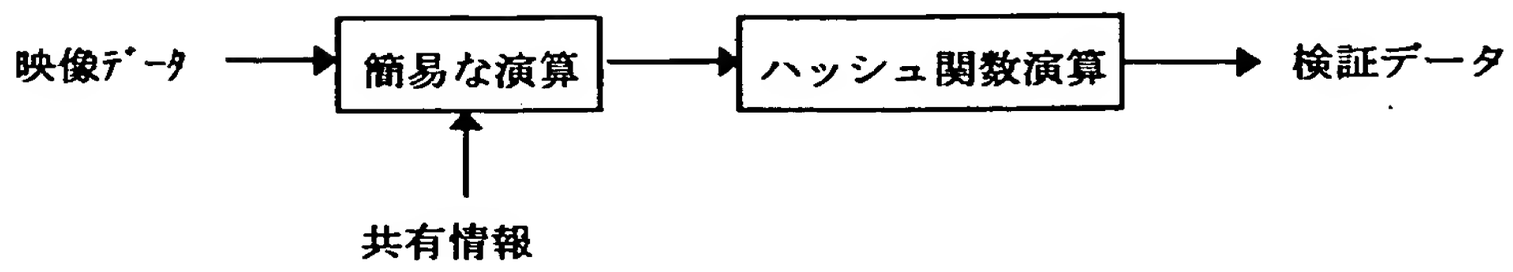


【図４】

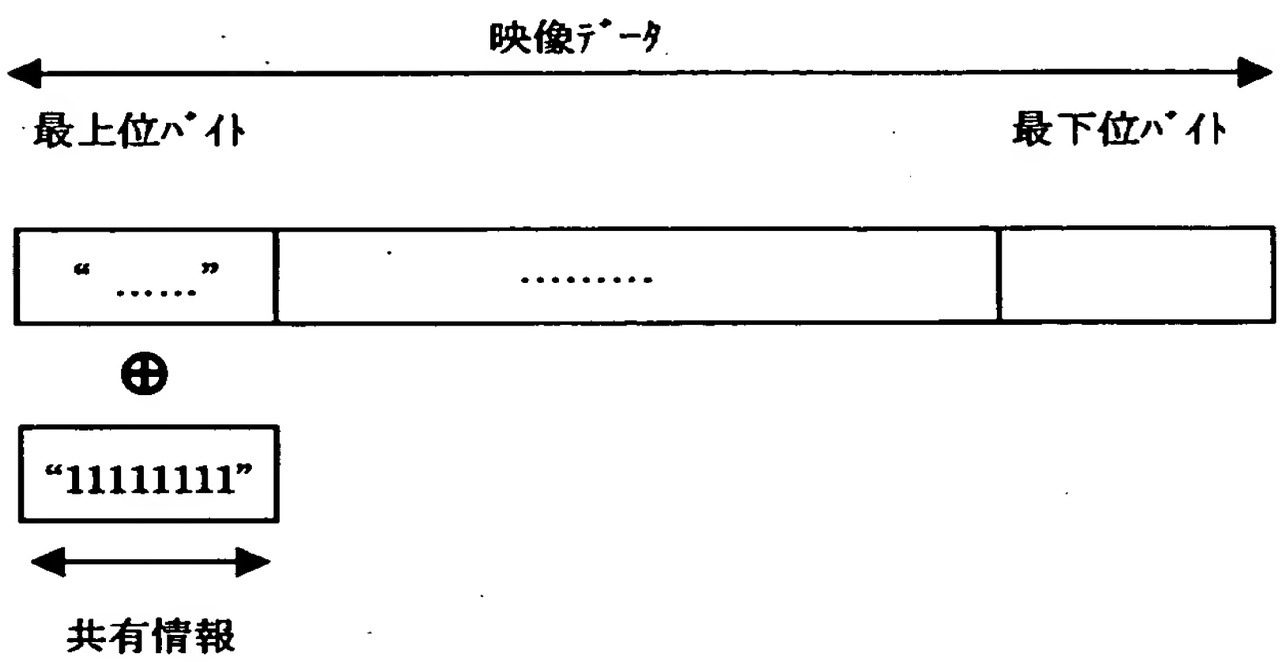


ID	ﾌｧｲﾙ名	登録日	検証日	公開鍵	経由	改竄
001	file1.jpg	2000/1/1	2000/1/2	PC1	PC1	無し
002	file2.jpg	2000/2/1	2000/2/2	PC2	PC2	あり
…	……	……	……	……	……	……

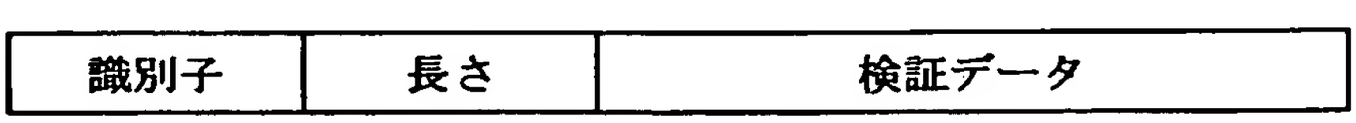
【図５】


映像ﾃﾞｰﾀ
簡易な演算
ハッシュ関数演算
検証データ
共有情報

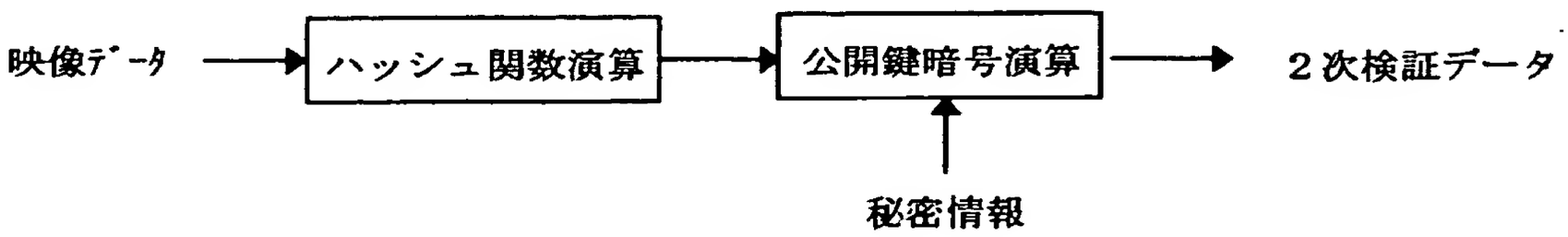
【図６】


映像ﾃﾞｰﾀ
最上位ﾊﾞｲﾄ
最下位ﾊﾞｲﾄ
“ ……”
……
⊕
“11111111”
共有情報

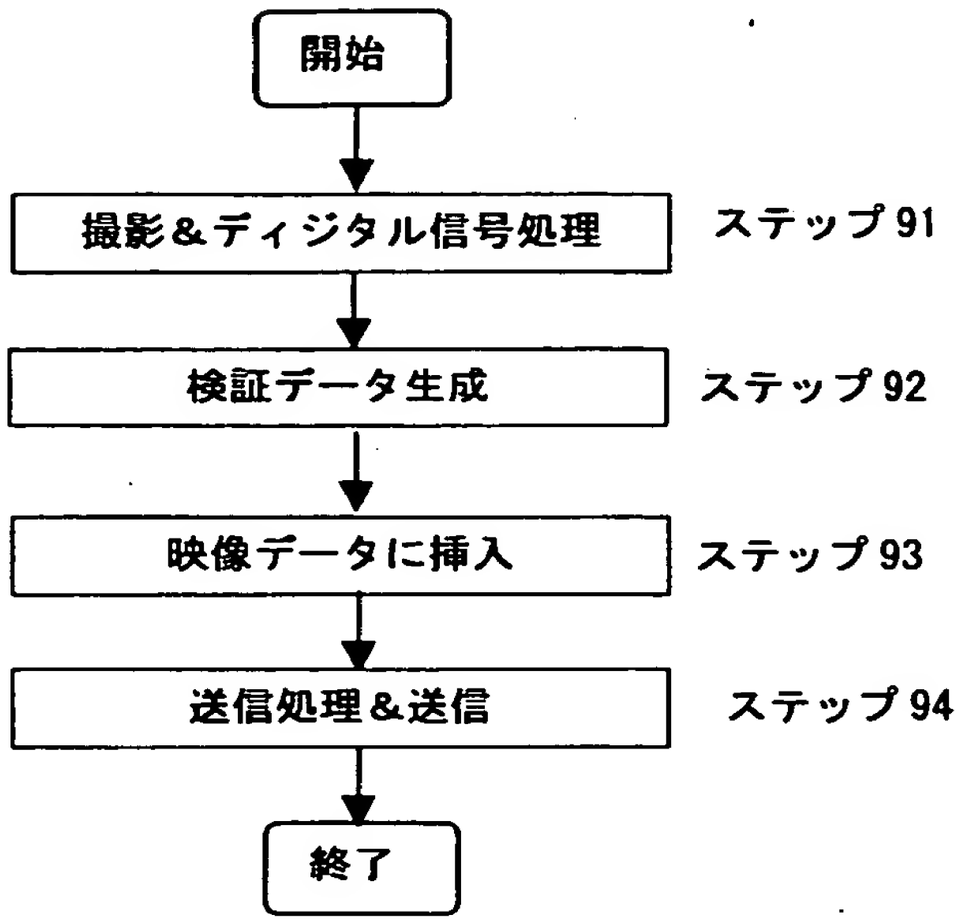
【図７】


識別子
長さ
検証データ

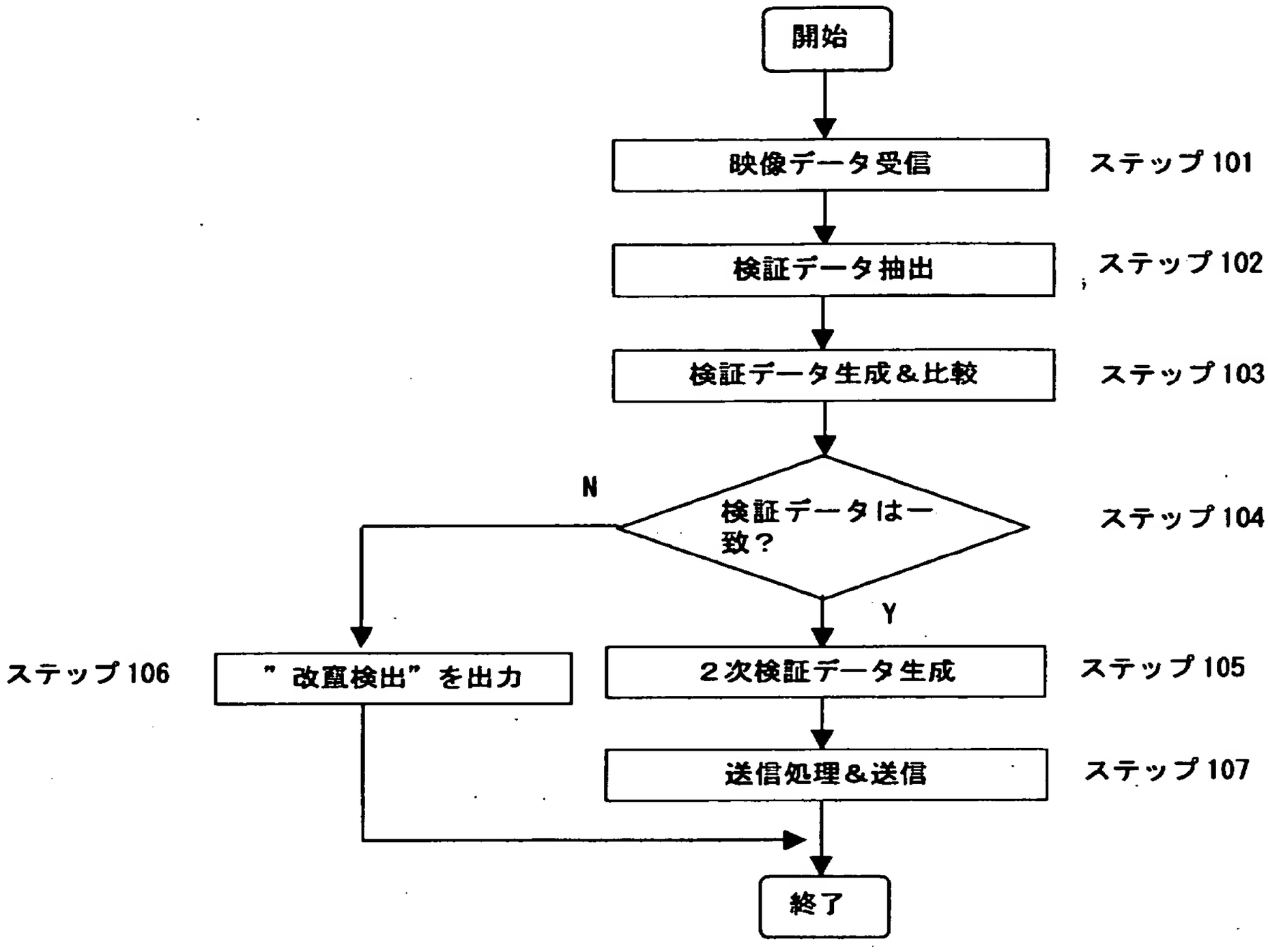
【図８】


映像ﾃﾞｰﾀ
ハッシュ関数演算
公開鍵暗号演算
２次検証データ
秘密情報

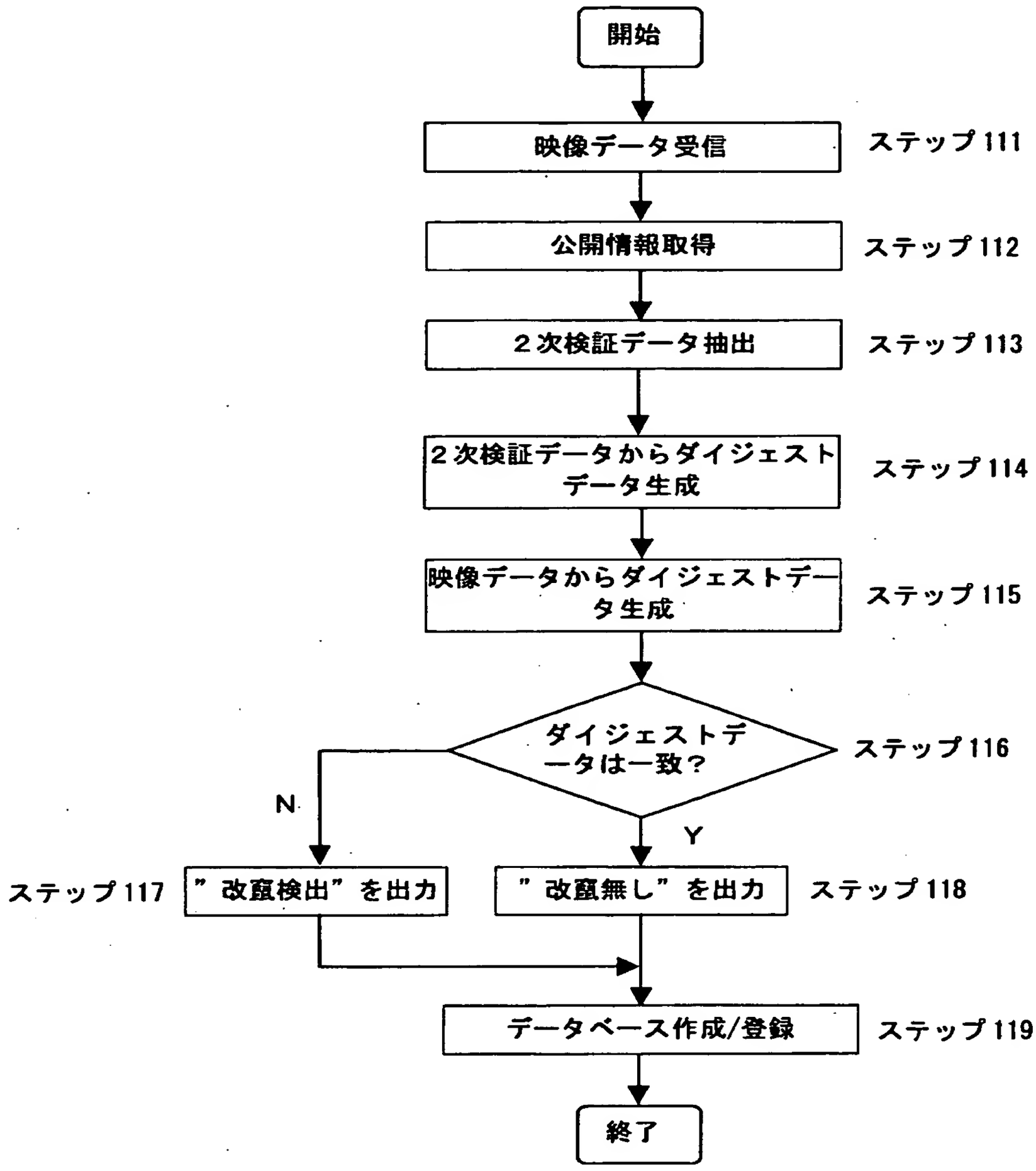
【図９】


開始
撮影＆ディジタル信号処理
ステップ91
検証データ生成
ステップ92
映像データに挿入
ステップ93
送信処理＆送信
ステップ94
終了

【図１０】


開始
映像データ受信
ステップ101
検証データ抽出
ステップ102
検証データ生成＆比較
ステップ103
検証データは一致？
ステップ104
N
Y
”改竄検出”を出力
ステップ106
２次検証データ生成
ステップ105
送信処理＆送信
ステップ107
終了

【図１１】


開始
映像データ受信
ステップ111
公開情報取得
ステップ112
２次検証データ抽出
ステップ113
２次検証データからダイジェストデータ生成
ステップ114
映像データからダイジェストデータ生成
ステップ115
ダイジェストデータは一致？
ステップ116
N
Y
ステップ117
”改竄検出”を出力
”改竄無し”を出力
ステップ118
データベース作成/登録
ステップ119
終了

【書類名】　　要約書

【要約】

【課題】　豊富な演算リソースを持たない映像入力装置の能力を向上させることなく、該映像入力装置にて撮影した映像データの完全性を保証するためのデータを生成することを課題とする。

【解決手段】　本発明の検証データ変換装置は、外部から入力される映像データと、該映像データの検証データと、映像データが生成された装置との間で共有する共有情報とに基づいて該映像データが改竄されていないかどうかを検証する検証処理部と、秘密情報を用いて該映像データから２次検証データを生成する検証データ生成部とを有する。

【選択図】　　図４

出　願　人　履　歴　情　報

識別番号　　〔０００００１００７〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社